Exhibit 3

Lease Accounting Audit Engagement Letter

Deloitte

Deloitte & Touche LLP
191 Peachtree Street, NE
Suite 2000
Atlanta, GA 30303-1943
USA

Tel: +1 404 220-1500
www.deloitte.com

February 22, 2018

Mr. Lewis Chew
Chair
The Audit Committee of PG&E Corporation
77 Beale Street
San Francisco, CA 94105

Mr. David S. Thomason
Vice President and Controller
PG&E Corporation
77 Beale Street
San Francisco, CA 94105

Dear Mr. Chew and Mr. Thomason:

This engagement letter is to confirm the engagement of Deloitte Risk and Financial Advisory1 ("Advisor" or "we" or "our" or "us") to provide PG&E Corporation and its subsidiaries (collectively, "PG&E", the "Client", the "Company" or "you") pre-implementation internal control assessment services in connection with the Client's planned changes in information systems and related business processes for the PowerPlant Lease Accounting module ("Lease Accounting System"), described below (the "Services").

Scope of Services

PG&E is in the process of implementing the Lease Accounting System across the organization. The Company is currently in the preparation stage of the implementation, performing user acceptance testing, training, among other activities.

The Services to be provided by Advisor are expected to consist of the following:

Obtain and analyze documentation provided by Client as well as hold discussion with relevant Client personnel in order to obtain an understanding of the following:

- The Client's design of controls for the Lease Accounting system for the following:
  - Finance / business process controls (manual and automated)
  - Interface controls (interfaces with key financial applications)
  - Controls over the completeness and accuracy of key reports (e.g., report logic, source data, and reporting parameters)
  - General information technology controls (e.g., security, change management)

---

1 As used in this engagement letter, "Deloitte Risk and Financial Advisory" means Deloitte & Touche LLP.

- The Client's project plan documentation supporting the implementation to understand and evaluate project governance / oversight (e.g., project charter, project plans, steering committee meeting minutes)

- The Client's User Acceptance Testing (UAT) (e.g. evidence of test scripts, test results, communication with UAT performers, Client's approval of testing) for system functionality and reports

- Client management's results of system testing and plans for "Go-Live" production validation to assess management's readiness for cutover to the Lease Accounting System

- Client management's controls over the reconciliation of data converted, as applicable, from source to destination systems. On a sample basis, analyze data converted from legacy systems to the Lease Accounting System in consideration of completeness and accuracy.

Based on upon the understanding obtained of the above, Advisor will consider this understanding in light of industry standards/leading practices and provide with high-level process and controls related advice and recommendations to management for PG&E's consideration.

The Services will be performed in accordance with the *Statement on Standards for Consulting Services* issued by the American Institute of Certified Public Accountants (AICPA).

Deliverables

Advisor's deliverables will consist of advice and recommendations for management's consideration. During this engagement, we may provide verbal and written comments and observations as well as potential recommended modifications to internal Client documents. Client management will be solely responsible to review and make all decisions with respect to potential modifications and ultimate approval and acceptance of any comments or observations made by Advisor.

Documentation and analyses prepared in connection with the Services shall merely represent the results of the engagement team's research and understanding of similar pre-implementation reviews performed in the industry and shall not represent an opinion of Advisor on any accounting or internal control position.

Under no circumstance shall Advisor prepare original documentation (e.g., accounting policies, internal control risk matrices or process narratives) that becomes part of the Client's records.

Inherent Limitations of an Entity's Internal Control

Because of the inherent limitations of internal control over financial reporting, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the

risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Engagement Team

Our engagement team will be composed of practitioners with experience in internal control over financial reporting (ICFR) and has been selected to align the team's skills with the technical and practical necessities of the engagement.

Name	Engagement Role	Title	
Tim Gillam	Lead audit partner	Partner	Deloitte & Touche LLP
Jay Cochran	Engagement Leader	Principal	Deloitte & Touche LLP
Patrick Giamanco	Senior Manager	Senior Manager	Deloitte & Touche LLP
Young Shim	Manager	Manager	Deloitte & Touche LLP

The engagement team will, as they consider necessary, call on other individuals with specialized knowledge and experience to assist in the performance of our Services, including professionals from our affiliate in India.

Fees and Timing

The Services are expected to be performed at the Client's offices in San Francisco, CA and remotely. Our engagement is expected to start as of May 1, 2018 and be completed by August 31, 2018.

Our hourly rates and professional fees reflect the complex, technical nature of the work to be performed and the need for experienced resources to perform this work. The professional fees for the engagement will be based on actual time incurred by each individual on the project and the respective rate for that level in the following table:

Resource Level	Hourly Rate
Partner/Managing Director	$365
Senior Manager	325
Manager	295
Senior	265
Staff	225
Offshore—India	100

Our preliminary estimate of our professional fees is based upon an estimate of 200 to 300 hours and ranges from $50,000 to $75,000, plus expenses. Please note this is only an estimate, as actual fees may vary. We will review our estimates periodically and inform you if there is a significant change in our estimate.

We understand that you will reimburse us for all reasonable expenses incurred in performing our Services on this engagement (including, but not limited to, our reasonable travel, meals, lodging, and mileage expenses).

Fees for this engagement will be billed monthly as the work progresses for fees accrued and expenses incurred since our last invoice in performing our Services.

Acknowledgments and Agreements

Client management acknowledges and agrees to the following:

- The performance of the services hereunder by Advisor is contingent upon the preapproval of this engagement letter by the Audit Committee of the Client in accordance with its preapproval requirements. Client management is responsible for the coordination of obtaining the preapproval of the Audit Committee, in accordance with the Audit Committee's preapproval process, for the Services to be provided by Advisor to the Client.

- Substantial and meaningful involvement of senior management of the Client is critical to the success of this engagement. The Client will be responsible for ensuring that the identified Client personnel actively participate in both the planning and execution of this engagement.

- The Services provided under this engagement letter should not be used as the sole basis for management's assertion in connection with the Sarbanes-Oxley Act of 2002 (the "Act"). Advisor will make no representations or warranties nor provide any assurances that (1) the Client's disclosure controls and procedures and the internal control and procedures for financial reporting are compliant with the certification requirement and internal control reporting requirement of the Act, or (2) the Client's plans are sufficient to address and correct any shortcomings that would prohibit the Client from making the required certification or from reporting under the Act.

- The Services will not constitute an engagement to provide audit, compilation, review, or attest services as described in the pronouncements on professional standards issued by the AICPA, the U.S. Public Company Accounting Oversight Board, or other regulatory body, nor an examination of management's assertions concerning the effectiveness of the Client's internal-control systems or an examination of compliance with laws, regulations, or other matters. Accordingly, our performance of the procedures will not result in the expression of an opinion or any other form of assurance on the Client's financial statements or any part thereof, nor an opinion or any other form of assurance on the Client's internal-control systems or its compliance with laws, regulations, or other matters.

- The Client is, and will continue to be, solely responsible for establishing and maintaining effective internal control over financial reporting, including, without limitation, systems designed to assure achievement of its control objectives and its compliance with applicable laws and regulations.

- Management is responsible for informing the Client's auditors and the Audit Committee of the Client's board of directors of all deficiencies in the design or operation of internal control over financial reporting, including separately disclosing all such deficiencies that

management believes to be significant deficiencies or material weaknesses in internal control over financial reporting. In addition, Advisor's personnel performing the Services may communicate directly to the Client's independent accountants such findings and information that have been previously communicated to the management of the Client.

- Advisor will not be responsible for the accuracy or completeness of any data made available to us through any third-party tool, database, or software application. The Company further acknowledges and agrees that Advisor will have no responsibility for evaluating the functionality of such third-party tool, database, or software application, nor for any results obtained by Advisor through the use of such third-party tool, database, or software application.

- Deliverables provided to the Client hereunder by Advisor may be disclosed by the Client to the Board of Directors of the Client only for their informational purposes and solely in their capacity as a member of such Board.

- Advisor will not conduct a legal review of any of the Client's documents, records, contracts, or policies. In addition, Advisor will not provide any legal advice regarding our Services nor will Advisor provide any assurance regarding the outcome of any future audit or regulatory examination or other regulatory action; the responsibility for all legal issues with respect to these matters, such as reviewing all deliverables and work product for any legal implications to the Client, will be the Client's.

- We will not perform in a capacity equivalent to that of management or an employee of the Client, including assuming any financial reporting oversight role; authorizing, executing, or consummating any transactions, or otherwise exercising authority on behalf of the Client or having the authority to do so; supervising employees of the Client in the performance of their activities; reporting to the board of directors on behalf of management of the Client; providing any legal advice with respect to, or conducting a legal review of, any documents, records, or policies of the Client; preparing source documents or originating data, in electronic or other form, evidencing the occurrence of any transactions; or recording of any amounts in books and records of the Client.

- The Client agrees that the Services may include advice and recommendations, but agrees that the Client will be solely responsible for the financial statements and all decisions regarding the accounting treatment of any item or transaction (including decisions regarding its compliance with U.S. GAAP). Furthermore, the Client shall be solely responsible for, among other things (1) designating a member of management with appropriate technical accounting and reporting knowledge to oversee the Services and to sustain meaningful and substantial involvement in all phases of this engagement; and (2) any forward-looking information (including any models, projections, forecasts, budgets, synergies, feasibility analyses, assumptions, estimates, methodologies, or bases for support). For the avoidance of doubt, we will be responsible for the performance of the Services.

During this engagement, the Client may request that Advisor perform additional services that are not encompassed by this engagement letter. Advisor may perform such additional services upon receipt of a separate signed engagement letter with terms and conditions that are acceptable to Advisor and the Client.

This engagement letter, incorporating by reference the attached General Business Terms in Exhibit A, and the other Exhibits attached hereto and incorporated herein by reference, constitutes the entire agreement between the Client and Advisor with respect to this engagement; supersedes all other oral and written representations, understandings, or agreements relating to this engagement; and may not be amended except by the mutual written agreement of the Client and Advisor.

Please indicate your acceptance of this agreement by signing in the space provided below and returning this engagement letter to us. A duplicate of this engagement letter is provided for your records.

Yours truly,

Deloitte & Touche LLP

By:
Jay Cochran, Principal

Accepted and Agreed to by
PG&E Corporation, on behalf of itself
and its subsidiaries:

By: David Thomason

Title: Vice President & Controller, Utility CFO

Date: 3/6/18

Accepted and Agreed to by
the Audit Committee of PG&E Corporation
and its subsidiaries:

By: Lewis Chew

Title: Chair, Audit Committee

Date: March 14, 2018

GENERAL BUSINESS TERMS

1. Services. The services provided by Deloitte Risk and Financial Advisory (the "Services") under the engagement letter to which these terms are attached (the "Engagement Letter") may include advice and recommendations, but Deloitte Risk and Financial Advisory will not make any decisions on behalf of Client in connection with the implementation of such advice and recommendations. For purposes of these terms and the Engagement Letter, "Client" shall mean the entity as defined in the Engagement Letter. PG&E Corporation represents and warrants that it has the power and authority to execute this agreement on behalf of, and to bind, itself and its subsidiaries.

2. Payment of Invoices. Client will compensate Deloitte Risk and Financial Advisory under the terms of the Engagement Letter for the Services performed and expenses incurred, through the term or effective date of termination of this engagement. Deloitte Risk and Financial Advisory's invoices are due upon receipt. If payment is not received within forty-five (45) days of receipt of an invoice (a) such invoice shall accrue a late charge equal to the lesser of (i) 1½% per month or (ii) the highest rate allowable by law, in each case compounded monthly to the extent allowable by law, and (b) Deloitte Risk and Financial Advisory may also suspend or terminate the Services. Client shall be responsible for any taxes imposed on the Services or on this engagement, other than taxes imposed by employment withholding for Deloitte Risk and Financial Advisory's personnel or on Deloitte Risk and Financial Advisory's income or property.

3. Term. Unless terminated sooner as set forth below, this engagement shall terminate upon the completion of the Services. Either party may terminate this engagement, with or without cause, by giving thirty (30) days' prior written notice to the other party. In the event of a termination for cause, the breaching party shall have the right to cure the breach within the notice period. Deloitte Risk and Financial Advisory may terminate this engagement upon written notice to Client if Deloitte Risk and Financial Advisory determines that the performance of any part of the Services would be in conflict with law, or independence or professional rules.

4. Deliverables.

   a) Deloitte Risk and Financial Advisory has rights in, and may, in connection with the performance of the Services, use, create, modify, or acquire rights in, works of authorship, materials, information, and other intellectual property (collectively, the "Deloitte Risk and Financial Advisory Technology").

   b) Upon full payment to Deloitte Risk and Financial Advisory hereunder, and subject to the terms and conditions contained herein, (i) the tangible items specified as deliverables or work product in the Engagement Letter (the "Deliverables") shall become the property of Client, and (ii) Deloitte Risk and Financial Advisory hereby grants Client a royalty-free, fully paid-up, worldwide, nonexclusive license to use the Deloitte Risk and Financial Advisory Technology contained in the Deliverables in connection with the use of such Deliverables. Except for the foregoing license grant, Deloitte Risk and Financial Advisory or its licensors retain all rights in and to all Deloitte Risk and Financial Advisory Technology.

   c) To the extent any Deloitte Risk and Financial Advisory Technology provided to Client hereunder constitutes inventory within the meaning of section 471 of the Internal Revenue Code, such Deloitte Risk and Financial Advisory Technology is licensed to Client by Deloitte Risk and Financial Advisory as agent for Deloitte & Touche Products Company LLC on the terms and conditions contained herein. The rights granted in this Section 4 do not apply to any Deloitte Risk and Financial Advisory Technology that is subject to a separate license agreement between Client and any third party (including Deloitte Risk and Financial Advisory's affiliates).

5. Limitation on Warranties. This is a services engagement. Deloitte Risk and Financial Advisory warrants that it shall perform the Services in good faith and with due professional care. DELOITTE RISK AND FINANCIAL ADVISORY DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. Client Responsibilities. Client shall cooperate with Deloitte Risk and Financial Advisory in the performance of the Services, including providing Deloitte Risk and Financial Advisory with reasonable facilities and timely access to data, information, and personnel of Client. With respect to the data and information provided by Client to Deloitte Risk and Financial Advisory or its subcontractors for the performance of the Services, Client shall have all rights required to provide such data and information, and shall do so only in accordance with applicable law and with any procedures agreed upon in writing. Client shall be solely responsible for, among other things (a) the performance of its personnel and agents; (b) the accuracy and completeness of all data and information provided to Deloitte Risk and Financial Advisory for purposes of the performance of the Services; (c) making all management decisions, performing all management functions, and assuming all management responsibilities; (d) designating a competent management member to oversee the Services; (e) evaluating the adequacy and results of the Services; (f) accepting responsibility for the results of the Services; and (g) establishing and maintaining internal controls, including monitoring ongoing activities. Deloitte Risk and Financial Advisory's performance is dependent upon the timely and effective satisfaction of Client's responsibilities hereunder and timely decisions and approvals of Client in connection with the Services. Deloitte Risk and Financial Advisory shall be entitled to rely on all decisions and approvals of Client.

7. Force Majeure. Neither party shall be liable for any delays or nonperformance directly or indirectly resulting from circumstances or causes beyond its reasonable control, including fire, epidemic or other casualty, act of God, strike or labor dispute, war or other violence, or any law, order, or requirement of any governmental agency or authority.

8. Independent Contractor. Each party hereto is an independent contractor and neither party is, nor shall be considered to be, nor shall purport to act as, the other's agent, partner, fiduciary, joint venturer, or representative.

9. Confidentiality and Internal Use.

a) All Services and Deliverables shall be solely for Client's benefit, and are not intended to be relied upon by any person or entity other than Client. Client shall not disclose the Services or Deliverables, or refer to the Services or Deliverables in any communication, to any person or entity except (i) as specifically set forth in the Engagement Letter, or (ii) to Client's contractors solely for the purpose of their providing services to Client relating to the subject matter of this engagement, provided that such contractors comply with the restrictions on disclosure set forth in this sentence. Client, however, may create its own materials based on the content of such Services and Deliverables and use and disclose such Client-created materials for external purposes, provided that, Client does not in any way, expressly or by implication, attribute such materials to Deloitte Risk and Financial Advisory or its subcontractors.

b) To the extent that, in connection with this engagement, either party (each, the "receiving party") comes into possession of any confidential information of the other (the "disclosing party"), it will not disclose such information to any third party without the disclosing party's consent, using at least the same degree of care as it employs in maintaining in confidence its own confidential information of a similar nature, but in no event less than a reasonable degree of care. The disclosing party hereby consents to the receiving party disclosing such information: (i) as expressly permitted in the Engagement Letter; (ii) to contractors providing administrative, infrastructure, and other support services to the receiving party and subcontractors providing services in connection with this engagement, in each case, whether located within or outside of the United States, provided that such contractors and subcontractors have agreed to be bound by confidentiality obligations similar to those in this Section 9(b); (iii) as may be required by law or regulation, or to respond to governmental inquiries, or in accordance with applicable professional standards or rules, or in connection with litigation or arbitration pertaining hereto; or (iv) to the extent such information (a) is or becomes publicly available other than as the result of a disclosure in breach hereof, (b) becomes available to the receiving party on a non-confidential basis from a source that the receiving party believes is not prohibited from disclosing such information to the receiving party, (c) is already known by the receiving party without any obligation of confidentiality with respect thereto, or (d) is developed by the receiving party independently of any disclosures made to the receiving party hereunder. In addition, any such information may be used by Deloitte Risk and Financial Advisory in the context of responding to its professional obligations as the independent accountants for Client. Nothing in this Section 9(b) shall alter Client's obligations under Section 9(a). Deloitte Risk and Financial Advisory, however, may use and disclose any knowledge and ideas acquired in connection

with the Services to the extent they are retained in the unaided memory of its personnel. Deloitte Risk and Financial Advisory shall promptly notify the Client if Deloitte Risk and Financial Advisory becomes aware of any unauthorized access to or disclosure of confidential information of the Client.

Third Party Information Technology Controls Reports. Deloitte LLP ("Deloitte U.S.") has engaged a third party (the "Service Provider") to (i) apply procedures based upon a version of the BITS Financial Institution Shared Assessment Program Agreed Upon Procedures with respect to certain of Deloitte U.S.'s information technology controls and to prepare a report with respect thereto (the "Shared Assessment Report"), and (ii) conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability, established by the American Institute of Certified Public Accountants (AICPA) ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC 2 Report"). Upon written request, Deloitte U.S. shall promptly provide Client with one copy of (i) the Shared Assessment Report, provided that Client executes any documentation required by the Service Provider to become a specified user thereof, (ii) the SOC 2 Report, or (iii) a report prepared by a third party that is designed to provide similar information as such reports. Client shall not disclose such reports, or refer to such reports in any communication, to any person or entity other than Client. In the event that Client has any questions regarding such reports, Deloitte U.S. shall make appropriate personnel reasonably available to discuss the contents thereof.

10. Survival and Interpretation. All provisions that are intended by their nature to survive performance of the Services shall survive such performance, or the expiration or termination of this engagement. For purposes of these terms and the Engagement Letter, "Deloitte Risk and Financial Advisory" or "Advisor" shall mean Deloitte & Touche LLP. Affiliated and related entities of Deloitte Risk and Financial Advisory are intended third-party beneficiaries of these terms, and may in their own right enforce such terms. Each of the provisions of these terms shall apply to the fullest extent of the law, whether in contract, statute, tort (such as negligence), or otherwise, notwithstanding the failure of the essential purpose of any remedy. Any references herein to the term "including" shall be deemed to be followed by "without limitation."

11. Assignment and Subcontracting. Except as provided below, neither party may assign any of its rights or obligations (including interests or Claims) relating to this engagement or the Services, without the prior written consent of the other party. Client hereby consents to Deloitte Risk and Financial Advisory subcontracting or assigning any portion of the Services to any affiliate or related entity, whether located within or outside of the United States; provided, however that such subcontracting will not relieve Deloitte Risk and Financial of any obligations to Client hereunder. Services performed hereunder by Deloitte Risk and Financial Advisory's subcontractors shall be invoiced as professional fees on the same basis as Services performed by Deloitte Risk and Financial Advisory's personnel unless otherwise agreed.

12. Dispute Resolution. Any controversy or claim between the parties arising out of or relating to these terms, the Engagement Letter, or this engagement (a "Dispute") shall be resolved by mediation or binding arbitration as set forth below.

a) Mediation. All Disputes shall first be submitted to nonbinding confidential mediation by written notice to the parties, and shall be treated as compromise and settlement negotiations under the standards set forth in the Federal Rules of Evidence and all applicable state counterparts, together with any applicable statutes protecting the confidentiality of mediations or settlement discussions. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR"), at the written request of a party, shall designate a mediator.

b) Arbitration Procedures. If a Dispute has not been resolved within 90 days after the effective date of the written notice beginning the mediation process (or such longer period, if the parties so agree in writing), the mediation shall terminate and the Dispute shall be settled by binding arbitration to be held in San Francisco, California. The arbitration shall be conducted in accordance with the CPR Rules for Non-Administered Arbitration that are in effect at the time of the commencement of the arbitration, except to the extent modified by this Section 14 (the "Rules").

The arbitration shall be conducted before a panel of three arbitrators. Each of Client and Deloitte Risk and Financial Advisory shall designate one arbitrator in accordance with the

"screened" appointment procedure provided in the Rules and the two party-designated arbitrators shall jointly select the third in accordance with the Rules. No arbitrator may serve on the panel unless he or she has agreed in writing to enforce the terms of the Engagement Letter (and its appendices) and to abide by the terms of this Section 12. Except with respect to the interpretation and enforcement of these arbitration procedures (which shall be governed by the Federal Arbitration Act), the arbitrators shall apply the governing law set forth in Section 16 in connection with the Dispute. The arbitrators shall have no power to award punitive, exemplary, or other damages not based on a party's actual damages (and the parties expressly waive their right to receive such damages). The arbitrators may render a summary disposition relative to all or some of the issues, provided that the responding party has had an adequate opportunity to respond to any such application for such disposition. Discovery shall be conducted in accordance with the Rules.

All aspects of the arbitration shall be treated as confidential, as provided in the Rules. Before making any disclosure permitted by the Rules, a party shall give written notice to all other parties and afford such parties a reasonable opportunity to protect their interests. Further, judgment on the arbitrators' award may be entered in any court having jurisdiction.

c) Costs. Each party shall bear its own costs in both the mediation and the arbitration; however, the parties shall share the fees and expenses of both the mediators and the arbitrators equally.

13. Non-exclusivity. Deloitte Risk and Financial Advisory may (a) provide any services to any person or entity, and (b) develop for itself, or for others, any materials or processes, including those that may be similar to those produced as a result of the Services, provided that Deloitte Risk and Financial Advisory complies with its obligations of confidentiality set forth hereunder.

14. Non-solicitation. During the term of this engagement and for a period of one (1) year thereafter, each party agrees that its personnel (in their capacity as such) who had substantive contact with personnel of the other party in the course of this engagement shall not, without the other party's consent, directly or indirectly employ, solicit, engage, or retain the services of such personnel of the other party. In the event a party breaches this provision, the breaching party shall be liable to the aggrieved party for an amount equal to thirty percent (30%) of the annual base compensation of the relevant personnel in his or her new position. Although such payment shall be the aggrieved party's exclusive means of monetary recovery from the breaching party for breach of this provision, the aggrieved party shall be entitled to seek injunctive or other equitable relief. This provision shall not restrict the right of either party to solicit or recruit generally in the media.

15. Entire Agreement, Amendment, and Notices. These terms, and the Engagement Letter, including attachments, constitute the entire agreement between the parties with respect to this engagement; supersede all other oral and written representations, understandings, or agreements relating to this engagement; and may not be amended except by a written agreement signed by the parties. In the event of any conflict or ambiguity between these terms and the Engagement Letter, these terms shall control. All notices hereunder shall be (a) in writing; (b) delivered to the representatives of the parties at the addresses set forth in the Engagement Letter, unless changed by either party by notice to the other party; and (c) effective upon receipt.

16. Governing Law and Severability. These terms, the Engagement Letter, including attachments, and all matters relating to this engagement shall be governed by, and construed in accordance with, the laws of the State of California (without giving effect to the choice of law principles thereof). If any provision of these terms or the Engagement Letter is unenforceable, such provision shall not affect the other provisions, but such unenforceable provision shall be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permissible the intent of the parties set forth herein.

17. Code of Ethics and Professional Conduct. We acknowledge that we maintain a Code of Ethics and Professional Conduct. The Deloitte Risk and Financial Advisory Code of Ethics and Professional Conduct (the "Code") may be found on www.deloitte.com under the Code of Ethics and Professional Conduct section under the Ethics & Independence section under the About section on that web site. The Code states that it is the obligation of all Deloitte Risk and Financial Advisory personnel to know, understand, and comply with this Code.

18. Background Check Contract Requirements. Deloitte LLP and its subsidiaries (collectively the "Deloitte U.S. Firms") generally require that background investigations be conducted for all employees, partners, and principals at the time that they join the Deloitte U.S. Firms. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of such factors as whether the issues identified are job related or pose a risk to the Deloitte U.S. Firms or to their respective employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining one of the Deloitte U.S. Firms is a partner, principal or employee, and the level of the employee. While background investigations were not always performed on Deloitte U.S. Firms' personnel, and may not always have covered the same information, all background investigations of Deloitte U.S. Firms' personnel in the U.S. currently include the following, at a minimum:

- SSN verification: confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:
  - Federal courts
  - County courts
  - State repositories, where the state has made one available and it is reasonably accessible
- A national criminal record database search, including the state sex offender registries.
- Education confirmation: all education beyond high school confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

19. Information Security: Deloitte Risk and Financial Advisory will comply with its security policies as set forth in Exhibit B.

EXHIBIT B

INFORMATION SECURITY STATEMENT

This Exhibit B is part of the engagement letter dated February 22, 2018, between Deloitte & Touche LLP and PG&E Corporation, and acknowledged and agreed to by the Audit Committee of PG&E Corporation.

Overview

Deloitte LLP and/or its affiliates ("Deloitte") have developed and implemented an Information Technology ("IT") infrastructure that is designed to generally align with industry standards. The security boundary of the IT infrastructure includes Deloitte- issued laptops, as well as infrastructure and applications, such as databases, document collaboration, email, and backup systems. The IT infrastructure security controls and associated information security processes were developed to protect confidential information while making it available in appropriate circumstances. A summary of such policies, controls, and associated processes is set forth below. From time to time, Deloitte may modify or update these policies, controls and associated processes. Deloitte shall not be under any obligation to notify any client of any such change to its policies, controls and associated processes.

Purpose

The purpose of this Information Security Statement is to provide an overview of Deloitte's IT security practices that are in effect as of the recent published date of this document.

Cyber Security

Deloitte's Chief Information Security Officer ("CISO") oversees the Cyber Security team, which provides assistance in the following areas:

- eDiscovery Forensic Investigations:
  - Manages the end-to-end process of collecting data requested by the Office of General Counsel ("OGC") for legal and regulatory matters
  - Works with OGC and the Talent organization to conduct internal investigations on misuse of data resources and manages security incident responses
  - Acquires, documents, and preserves digital evidence for computer forensics
- Risk & Compliance:
  - Leads and manages the vendor security program and privacy impact assessment process
  - Collaborates with client service leaders and OGC in responding to client security inquiries and security agreements
  - Leads Deloitte's third party audit and assessment (e.g., SOC2 and Shared Assessments Agreed Upon Procedures)

- Leads Deloitte's security awareness efforts and assists with global security awareness efforts
- Responsible for exceptions to security policies and standards

- Cyber Defense:
  - Monitors, analyzes, and responds to all types of system, device, and application events, such as user activity, firewalls, IDS/IPS, antivirus, and vulnerabilities
  - Identifies, rates, and remediates potential security vulnerabilities of applications and systems
  - Understands which Deloitte systems are used, how, and by whom and uses this information to protect the organization from potential threats
- Data Protection:
  - Reviews emerging technologies, security architecture, and proposals for improvements
  - Leads the identity management program
  - Leads Federal support and maintains FedRAMP certifications

Members of the Cyber Security team hold various industry security- and audit-based certifications (e.g., CISSP, CISM, CISA, ISSM, CRISC, CEH, ISO 27001 Lead Auditor, and OSCP).

Information Security Program

Deloitte maintains a comprehensive information security program, which includes policies, standards, procedures and guidelines. The information security program is informed by several industry-standard guidelines and best practices including ISO27002, COBIT, ITIL, American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC2"), and the Shared Assessments Program (formerly known as the "BITS Financial Institution Shared Assessments Program").

Deloitte's IT leadership meets on a regular basis to consider strategic and tactical direction for the information security program, and its policies, standards, procedures and guidelines.

Information security policies are drafted with input from internal information security stakeholders and are based upon industry standard practices. The drafts are reviewed and approved by Deloitte's Cyber Security leadership, OGC, the Office of Confidentiality and Privacy, the CISO and Deloitte's Chief Information Officer. Once approved, the policies are published on Deloitte's intranet and communicated to personnel.

On-Site Security Assessments

In an effort to protect and minimize risk to Deloitte's client data, in lieu of permitting individual clients to perform independent security assessments of Deloitte's information security program, each year Deloitte engages an independent third-party auditor ("Third Party") to (i) conduct an examination in accordance with AT Section 101 of the Statement

on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability established by the AICPA ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC2 Report"), and (ii) apply procedures based upon a version of the Shared Assessments Program Agreed Upon Procedures (the "Shared Assessments AUPs") with respect to certain of Deloitte's information technology controls and to prepare a report with respect thereto (the "Shared Assessments Report").

Soc2 Report

The SOC2 Report includes the Third Party's opinion on the fairness of the presentation of the description of Deloitte's systems in management's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on the Third Party's examination. The SOC2 Report also includes a description of Deloitte's systems and controls, and a description of the Third Party's criteria, test procedures, and the results of such tests. The SOC2 Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the SOC2 Report.

Shared Assessments Report

The Shared Assessments Report is used to assist Deloitte management in evaluating certain IT controls related to the security of Deloitte's client data. The Shared Assessments Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the Shared Assessments Report and has executed an access letter with the Third Party.

The Shared Assessments Program includes the Agreed Upon Procedures (which are a list of security control objectives) and the Standardized Information Gathering ("SIG") questionnaire. Detailed information about the Shared Assessments Program can be found at http://www.sharedassessments.org/. The Shared Assessments Program defines specific controls and objectives as well as the procedures for verifying those controls. The Agreed Upon Procedures address the following controls areas:

- Risk management
- Information security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance
- Privacy

Awareness and Training

Deloitte has implemented training and awareness programs for its personnel related to information-security, confidentiality and privacy policies, and data-protection standards. All Deloitte personnel are required to complete information security awareness training during

the new-hire onboarding process. All personnel are presented with an information security policy awareness statement via Deloitte's intranet two times each year, which they are required to acknowledge within two weeks of the statement's release.

Deloitte personnel are also required to complete a confidentiality, privacy and information security training course.

Deloitte has a dedicated security awareness committee. The committee is responsible for developing ideas to enhance Deloitte's awareness of security risks and issues through policy development and training. The committee is comprised of delegates from Deloitte's Cyber Security leadership, National Office of Security, Office of Confidentiality and Privacy, CISO, National Quality Risk Management, Talent, and OGC, and from Deloitte Touche Tohmatsu Limited's Global Information Security Office, who regularly meet to discuss new or recurring security issues, devise strategies and implementation plans, and provide progress reports on existing projects.

Management and Protection of Confidential Information

Deloitte is committed to protecting the confidential information of our clients, our organization and the third parties with whom we work. "Confidential Information" refers to any information not generally available to the public, in any form, that Deloitte receives or creates in the course of business. To support this commitment, Deloitte has established the Office of Confidentiality and Privacy and developed the "Confidential Information Program" for proactive management and protection of Confidential Information. The Office of Confidentiality and Privacy is responsible for setting guidelines, developing procedures, and providing consultation and training on the management of Confidential Information. The Office of Confidentiality and Privacy is also responsible for implementing the Confidential Information Program across Deloitte.

The Confidential Information Program consists of processes, technology controls, training, and communications that help our professionals to improve their awareness of risks associated with Confidential Information and their ability to properly manage and safeguard Confidential Information.

The Confidential Information Program

The Confidential Information Program consists of processes and activities that are performed throughout the engagement lifecycle to manage and protect Confidential Information.

Client account and engagement teams in the Confidential Information Program generally do the following:

- Appoint a data manager responsible for overseeing program activities;
- Develop and maintain a Confidential Information management plan to document the Confidential Information management strategy and safeguards employed;
- Develop and deliver Confidential Information onboarding training that outlines the protocols that team members must follow when accessing, storing, using, transferring, and disposing of Confidential Information;

- Implement physical, administrative, and technical safeguards identified in the Confidential Information management plan to proactively manage risk; and

- Complete all other required confidentiality training as applicable.

The Confidential Information Program also includes an insider threat program in which Deloitte conducts active monitoring of external as well as insider threats. Insiders are defined as personnel and contractors who, based on their access to certain systems and information, could adversely affect the brand, reputation and/or business of Deloitte or its clients. Leveraging potential risk indicators, the insider threat program monitors persons of interest across a broad risk spectrum, including workplace violence, espionage, fraud, and theft of intellectual property and confidential information. Analytic and cognitive technologies are used to help identify indicators of poor risk-culture fit and determine corresponding strategic tactics and mitigation strategies to align our sub-cultures.

Data Privacy

Data Privacy is a key function of the Office of Confidentiality and Privacy. Deloitte has a data privacy policy, applicable procedures, and personnel dedicated to making sure we are in compliance with applicable data privacy laws and regulations.

- Deloitte has policies and procedures that protect personally identifiable information ("PII") and support compliance with US and the European Union (EU) legal requirements relating to the transfer and processing of PII, including personal health information. Deloitte adheres to the Privacy Shield Framework with respect to PII that is transferred from the European Economic Area to the United States.

- Deloitte is not a "Covered Entity" as defined under the Health Insurance Portability and Accountability Act, as amended ("HIPAA"). Therefore, Deloitte is generally not required to, and does not, comply with the obligations of a Covered Entity. However, when Deloitte acts in the capacity of a "Business Associate" to our clients, as such role is defined under HIPAA, Deloitte is required to comply with the obligations of a Business Associate under HIPAA. Deloitte has implemented policies, procedures, and controls that facilitate compliance with those obligations.

- Deloitte has instituted an annual review process across all Deloitte business areas to verify compliance with privacy policy and procedures.

Confidentiality and Privacy Incident Management

Deloitte has instituted an integrated incident response process designed to facilitate prompt reporting and resolution of incidents. Our confidentiality and privacy incident response process is characterized by the following:

- Centralized reporting of actual or suspected incidents to a Help Desk, which is available 24/7 with access via a toll-free number;

- Training and awareness programs focused on helping personnel understand immediate steps to be taken in case of actual or suspected incidents;

- Established roles and responsibilities for incident management and response including involving the appropriate consultation resources across the Deloitte organization, as applicable to the specific matter;

- Documented processes to help gather incident facts, initiate response activities, engage incident response teams, escalate incidents and alert appropriate leaders, based on the nature of the specific incident;
- Consultation among the relevant parties regarding the need for a corrective action plan;
- Development, as appropriate, of action plans, including any required communications, as well as actions to mitigate the risk of a future recurrence; and
- Post-incident follow-up process to analyze root causes and integrate lessons learned.

IT Continuity Management

Deloitte maintains an active disaster recovery and business continuity program which helps to continue delivering information-technology-related services should a disruption occur. Deloitte's program includes the following basic activities:

- Business continuity planning for IT infrastructure support staff;
- Business impact assessments to help define criticality of processes and systems related to recovery time objectives;
- Disaster recovery planning of our technology through multiple failover capabilities;
- Implementation of resilient architectures where technology allows;
- Risk assessments as part of continual service improvement, with countermeasures identified and implemented for the newest scenarios; and
- Internal review process for maintaining the quality of plans and services.

The business continuity program ("BCP") and plans include emergency-response business procedures, which go into effect following the occurrence of a disaster or other unplanned interruption.

Disaster recovery ("DR") plans include technical and business contact call lists, as well as notification and escalation information and architecture diagrams. Where pertinent, third-party information is also included. Recovery time objectives and recovery point objectives are documented and tested for each plan.

BCP/DR plans are subject to review and testing every 12 months with industry standard testing methods.

Risk assessment test scenarios vary based on business sensing and technology security. Test results are reviewed and recorded.

In summary, Deloitte has a comprehensive disaster recovery and business continuity program that is designed to provide for the continuity of essential IT business functions and critical business processes following the occurrence of a disaster or other unplanned interruption impacting Deloitte's IT infrastructure.

Business Continuity Management

Deloitte takes disaster and contingency planning very seriously, including planning for events that impact its people and/or its facilities. Deloitte's business continuity planning addresses issues such as, communications, travel, resource allocation, technology needs, and alternate work sites. Response procedures assess the well-being of personnel, provide for the continuity of essential business functions, and utilize recovery procedures for the restoration of critical business processes.

Cross-functional teams are identified to manage potential disruptive events, emergency situations or disasters. Each Deloitte office has a local crisis management team to handle smaller, localized events impacting a single location. For larger events or those that are not specific to a single location or geography, an experienced national incident support team is assigned ("National Incident Support Team"). A national crisis council handles incidents that rise to the level of a true crisis requiring strategic involvement and decision-making.

Cross-functional teams are identified and documented in the plans to include representation of key stakeholders from the following areas:

- Client Services
- Office Services/Operations/Facilities
- Office of Security
- Human Resources and Benefits
- Information Technology Services
- Procurement and travel
- Communications
- Risk Management

Deloitte has designed an impact-driven approach, which focuses on the impacts of an event, emergency, or crisis, rather than specific scenarios. Each type of situation could have an impact on our people, our facilities, our technology, or our clients. Each type of situation could require communications, whether internal or external. The team-based, impact-driven approach utilized by Deloitte provides the best resources to assess and address the impacts of an event.

Deloitte has developed a specific plan to address the impacts and continuity of operations in light of a pandemic ("Pandemic Plan"). The Pandemic Plan and related governance model is aligned with the crisis management and business continuity processes, including the use of the National Incident Support Team, but is supplemented by additional members of a Pandemic Response Committee. The Pandemic Response Committee monitors potential pandemic developments, and would oversee implementation of specific pandemic action steps based on the severity of the pandemic, including targeted communications that would be issued internally and externally, and identification of critical people and resources.

Limits of Business Continuity and Pandemic Planning

Due to the significant uncertainties associated with a possible flu pandemic or other disaster, Deloitte can make no representations or warranties, nor provide any assurances, that its plans will be adequate to respond to any possible consequences, or that the plans of any third parties to deal with a possible flu pandemic or other disaster are or will be sufficient to address any situations or problems that might arise during a pandemic or other disaster. Deloitte's objective is to prepare for a possible flu pandemic or other disaster

based on the information and data that it has at this time, and to possibly modify those plans as it believes conditions or facts may warrant.

Every organization needs to develop its own preparedness plan based on its specific circumstances, business functions, and operational factors. Consequently, a plan developed for one function or business cannot be expected to address the potential issues that may be faced by another business enterprise. Because business continuity and disaster recovery plans and documentation contain information about Deloitte that is proprietary and confidential, Deloitte does not provide third parties with copies of such plans or documentation.

Human Resources Security

Upon hire, all personnel agree to comply with Deloitte's policies, including those relating to information security, confidentiality and privacy. In addition, all Deloitte personnel are required to complete security awareness training during the new hire onboarding process.

Background Checks for U.S. Personnel

Deloitte generally requires that background investigations be conducted for partners, principals and all employees at the time that they join Deloitte. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of whether the issues identified are job-related or pose a risk to Deloitte or to its employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining is a partner or principal and the level of the employee. While background investigations were not always performed on Deloitte personnel, and may not always have covered the same information, all background investigations of Deloitte personnel in the U.S. currently include the following, at a minimum:

- SSN verification: confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:
  - Federal courts
  - County courts
  - State repositories, where the state has made one available and it is reasonably accessible
- A national criminal record database search, including the state sex offender registries.
- Education confirmation: education beyond high school confirmed
- Employment confirmation: professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.

- Professional licenses: confirm relevant professional licenses

Recurring Background Checks for U.S. Personnel

In addition to the background checks described above, Deloitte currently requires that additional criminal background checks be conducted at five-year service intervals for all Deloitte personnel in the U.S.

Background Checks for Personnel of Deloitte Entities Located In India ("U.S. India")

The type of background investigation performed depends on whether the individual joining U.S. India is a partner, principal, or employee, and the level of the employee. While background investigations were not always performed on U.S. India's personnel and may not always have covered the same information, all background investigations of U.S. India personnel currently include the following, at a minimum:

- Identity Verification, where possible
- Criminal checks: check all relevant court records for a five year period
- Education confirmation: all university level education is confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, including India specific and global databases
- Professional licenses: confirm relevant professional licenses

Physical and Environmental Security

Only authorized personnel with a Deloitte-issued electronic badge are granted access to Deloitte's facilities. Procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the facilities. Deloitte data centers are further restricted to only those personnel with the need to access restricted areas. Data centers have the following physical security measures: security guards, man-trap doors at primary entrance, multi-factor authentication (Deloitte-issued electronic badge and biometric readers) at secondary entrance, video cameras, and sign-in and sign-out sheets for escorted visitors.

The electricity, water, and temperature controls are all pre-approved for use by the facilities administrators in the data centers. Each utility has a control in place to monitor its usage and to notify an administrator in case of failure. Automatic emergency lighting is installed in areas necessary to maintain personnel safety.

Emergency exits are located in appropriate places in Deloitte facilities. Automatic fire suppression systems have been installed to protect the facilities. In data centers, the primary system is HFC-125 chemical based and activated via multiple smoke detectors, and the second type is pre-action hydronic, and the detection method is temperature. Master water shut-off valves are present. Temperature and humidity controls have been implemented to protect against temperature fluctuations in all areas of the data centers containing IT equipment.

Risk Management

Deloitte has a risk management program that monitors possible threats and vulnerabilities to information technology assets. Risk assessment(s) are performed annually and when there are significant changes to infrastructure, technology or environment. There are several control domains defined for risk assessment. These control domains are derived from industry standard practices and frameworks. For each control domain, implemented controls are identified and tailored and their effectiveness assessed for risk management. Risks that are not at an acceptable level are remediated or mitigated.

Vendor Hosting and Processing

Deloitte has arrangements with vendors who provide Deloitte with certain software-as-a service and hosting services. Deloitte selects and retains these vendors based on, among other qualities, their capability to maintain safeguards for the systems, software and information at issue that are consistent with leading industry security practices. Deloitte requires these vendors to implement and maintain such safeguards.

Vendor Assessment Process

The Vendor Assessment process is designed to reduce vendor-related risk by:

- Building a repository of acceptable vendors;
- Assessing the security posture of vendors;
- Tracking remediation of identified issues; and
- Reviewing and assisting with vendor contracts with respect to obligations relating to Deloitte's information security program.

Asset Management

Deloitte has an asset management team that is responsible for oversight and management of Deloitte assets and inventory throughout its lifecycle. There are tools and controls in place that manage all hardware and software assets. Deloitte has policies and procedures in place to manage licensed software and security controls to deter prohibited software from being installed and/or used. A software and hardware inventory system is maintained, which identifies hardware and software components used within Deloitte information systems. Multiple controls are used to manage the configuration baselines, including mobile device management. These controls are supported by automated tools that provide configuration and inventory information on a continuous basis specific to configuration compliance, known vulnerabilities, inventory by Internet Protocol address ("IP address")/device name and asset operational and connection status.

Access Control

Access to Deloitte information contained on Deloitte IT systems is granted on a need-to-know basis and must be approved by the Deloitte data owner.

Vendor and contractor access is requested through formal procedures that involves Deloitte's Talent and Technology groups. Upon approval, the vendor user accounts are created in a controlled domain organizational unit giving the access necessary to perform

their defined duties. Vendor and contractor access is granted on a temporary basis requiring regular review and renewal of approval by management.

For certain systems remote access is provided via a Secure Sockets Layer ("SSL") Virtual Private Network ("VPN") using two-factor authentication with account activity being logged to Deloitte's logging/alerting mechanism. Depending on the level and type of access required, the SSL VPN solution provides a virtual session or web interface with access into the needed application(s) or platform.

Web-based applications that contain or provide access to sensitive internal or client data (including VPN), multi-factor authentication (MFA) has been enabled. Verification options include phone call, text message, or mobile application.

Privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into role-based groups (e.g., key management, network, system administration, database administration, and web administration).

Identification and Authentication

All users must authenticate to the Deloitte network using a unique user identification ("ID") and a strong password prior to gaining access to the information system.

Deloitte strong passwords contain the following characteristics:

- At least ten characters in length
- Cannot be any of 24 previous passwords
- Expire every 90 days
- Lockout threshold after 6 invalid logon attempts
- Contain at least three of the following four classes:
  - English uppercase letters (A, B, C,...)
  - English lowercase letters (a, b, c,...)
  - Westernized Arabic numerals (0, 1, 2,...)
  - Non-alphanumeric (special) characters (#, &, !, %, @,?,*, et al.)

System Security

System and Communications Protection

An intrusion prevention system ("IPS") is employed at the point of entry to the Deloitte network environment. The logs for the IPS, firewall, and VPN are sent to a log aggregator. Access control lists are placed on firewalls controlling the inbound and outbound flow of traffic. Traffic is denied by default unless approved by the gateway protocols as configured

and approved by the Deloitte security team. A demilitarized zone ("DMZ") and trusted zones are used to segment traffic to areas that are protected in accordance with the accepted risk levels.

System and Information Integrity

Firewall, IPS, and VPN audit logs are sent to the log aggregator, which checks for abnormal activity and anomalous behavior that would trigger an information security review. Hardware and software checks are done by automated tools with identified alert levels that trigger a notification to the system administrators in case of a system flaw. Anti-virus and malware protection is managed by enterprise policy and distributed by a server located in the environment periodically. Anti-virus is configured to scan external devices attached to the information system as well as email traffic.

Data Back-up

Deloitte systems are scheduled for daily backup and two iterations of data through redundant data mirroring: one onsite and one offsite. If a system backup is interrupted for any reason, it will resume on the alternate site where it left off. A reputable vendor is utilized for offsite backup storage and disposal. All backup media is encrypted prior to shipment to the vendor and a controlled process exists for turnover. The vendor is subject to obligations of confidentiality. The vendor has security practices in place and uses a tracking application for all media it handles on Deloitte's behalf. Deloitte is provided with inventory reports of the media and chain-of-custody. The vendor stores the media in a secure, environmentally-controlled storage facility.

Information Systems Acquisition, Development and Maintenance

Security Planning

The Deloitte information security program, applicable policies, standards, standard operating procedures and guidelines are reviewed annually and updated as necessary.

Acquisition of System and Services

Deloitte does not acquire IT systems or services until Cyber Security has reviewed the product or service to determine whether it meets internal guidelines with respect to security and encryption. Software installation requests are submitted for risk assessment and approval. Software is not implemented unless it meets applicable Information Technology Services ("ITS") standards. There is a Change Control Board ("CCB") that discusses any changes that may affect the security posture of the environment and documents all proposed upgrades or modifications to the environment, assets and infrastructure.

Application Development

Deloitte follows secure coding best practices during the system development lifecycle for Deloitte applications. Deloitte's applications undergo security reviews, testing and vulnerability scans prior to being placed in production.

Change Control

Deloitte has a change management process in place for its IT systems. Proposed changes are submitted, tested, and reviewed during regularly scheduled CCB meetings. Approved

changes are tested and vulnerability scans are performed prior to deployment. Deployment windows are scheduled to minimize the impact to Deloitte's operations. Back-out plans are in place should they be needed.

Patch Management

Deloitte has a patch-management program and supporting tools in place that are managed by an internal patch management team ("PMT"). Vendor and industry-accepted alert lists are monitored for new patches. Patches are reviewed by the PMT at regularly scheduled meetings and are rated for deployment based on assessed severity levels. Emergency patch management meetings are called when needed.

Vulnerability Management

Deloitte's network undergoes penetration testing and vulnerability scans performed by Deloitte 's Cyber Defense team. Penetration tests are performed annually on the network infrastructure's external perimeter by Deloitte's Cyber Defense team. Vulnerability scanning is performed weekly on the network infrastructure's external perimeter by Deloitte's Cyber Defense team. Vulnerability scanning is performed monthly on IT infrastructure's internal network by Deloitte's Cyber Defense team.

Maintenance

Deloitte ITS performs software and hardware maintenance on Deloitte's environment servers.

Information system backups are performed daily. Performance reports are initiated through automated tools that specify certain levels of performance to trigger the generation of the report (i.e., % of CPU processor utilization, etc.).

Third-party contractor maintenance personnel must be approved prior to receiving access to the information system servers. Third party maintenance personnel are escorted into the facility and accompanied during the period of access. A log is maintained which documents the name, date, length of time, justification, and escort name for each maintenance individual who is granted access to the information system(s).

Information Security Incident Management

Deloitte has built an integrated incident response team that brings together the appropriate subject matter experts from various cross-functional disciplines to address each specific incident. The Security Incident Response Procedures ("Procedures") describe how various types of incidents are handled. The Procedures identify key resources and communications that will take place based on various incident types. The Procedures identify to whom suspected incidents should be reported and describe the escalation path from the entry point in the process through fruition. Security awareness training is in place to educate Deloitte personnel of their responsibilities concerning security incidents. Each incident is logged and the relevant facts are captured for analysis and reporting. When necessary, data related to the incident is maintained in a forensically sound manner and appropriate chain-of-custody is documented.

The incident response team has a variety of tools available to assist them in the analysis of incidents. These include standard security tools from software and hardware providers as well as commercial forensic tools specifically targeted for such matters.

Information security incident procedures are executed periodically so the teams remain prepared for response should the need arise. At the completion of each significant incident, a post-incident review is conducted to identify any areas for improvement as well as lessons learned. These findings are used to adjust, enhance or improve the procedures.

Compliance

System Audit and Accountability

System audit logs and records are created to monitor the following:

- anti-virus services
- intrusion prevention services
- remote access services, web proxy services
- domain authentication
- router events
- firewall events
- VPN access
- application logs

System audit logs are maintained to support analyses and investigations. Logs are maintained for a period of 180 days. Logs may also be preserved based on legal or regulatory requirements.

System audit log content includes: (i) date and time of the security event; (ii) the component of the information system (e.g., software component, hardware component) where the security event occurred; (iii) type of security event; (iv) unique user/subject identity; and (v) the outcome (success or failure) of the security event.

System Audits

Deloitte's internal audit team periodically performs internal audits on various aspects of Deloitte's systems, processes, and policies.

Application Configuration Management

Software baseline requirements are created in accordance with Deloitte policies and standards. Software is tested against the baseline requirements prior to being placed in the production environment. Continued monitoring and change management processes are conducted while in operation.

Wireless Access

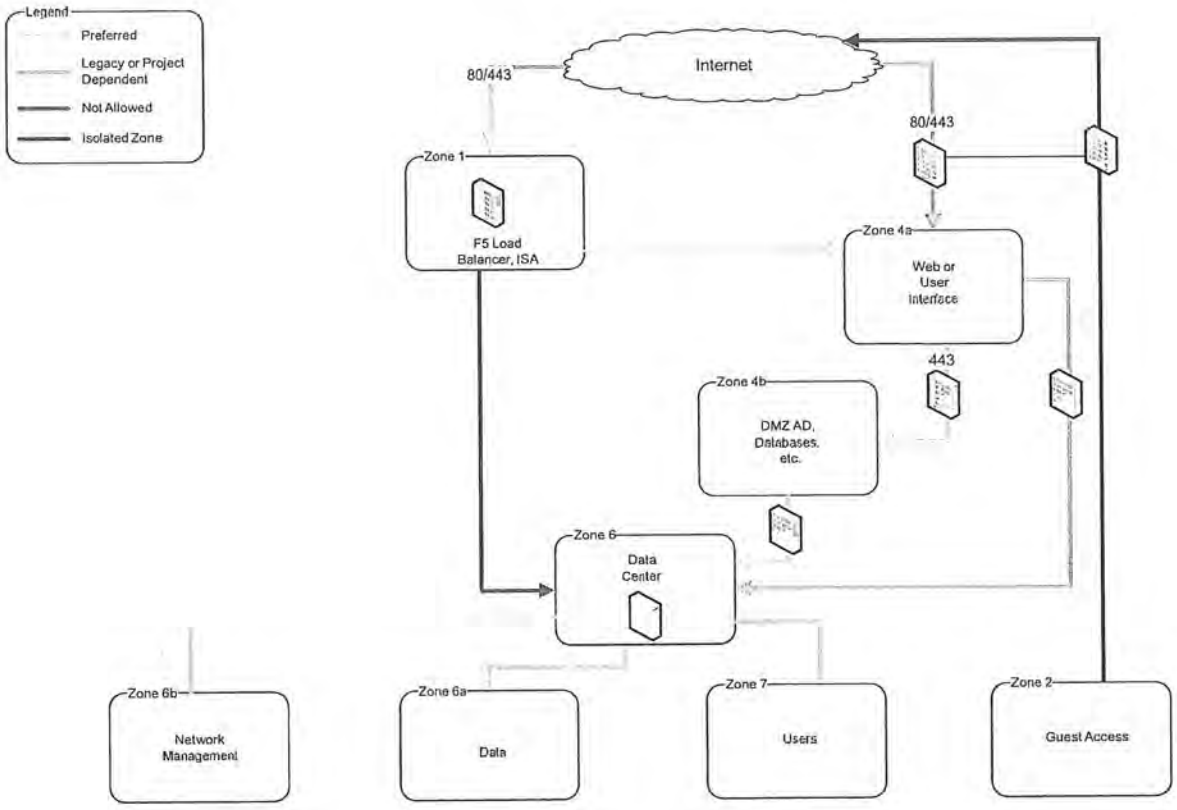
Deloitte supports an internal wireless network within the organization. A wireless-security and acceptable-use policy is in place. Only Deloitte-approved access points will be connected to Deloitte's network.

- For wireless access to Deloitte's networks, personnel are required to use Wi-Fi Protected Access (WPA2 or stronger protection) where it is available.

- For the convenience of visitors, clients, or guests, a guest wireless network providing controlled access to the Internet may be made available in Deloitte's facilities.

Data Flow Diagram

Zone Flow—Basic Rules for Zone Flow



Data Protection

PII

Deloitte personnel receive training on the proper handling of PII. In instances where Deloitte may transmit client PII outside of the Deloitte environment, Deloitte requires transmission of such data in an encrypted format.

Media Protection

Secure printing is available at multiple locations within each Deloitte office that requires the usage of a Deloitte-issued electronic smartcard badge to enable the print job. Further, Deloitte issues encrypted USB drives to its personnel that meet the encryption standards outlined in Federal Information Processing Standard ("FIPS") 140-2. In addition, software has been deployed to Deloitte-issued IT assets as part of the standard application toolset that allows the creation of encrypted WinZip files (FIPS 197 compliant).

Deloitte has implemented a technical control that encrypts data written/copied to external USB devices which can only be read by a Deloitte machine.

Laptops are encrypted and are required to be physically secured at all times. Physical access to servers is restricted to authorized parties. Magnetic drives are wiped/over-written with a minimum of three passes with a media sanitization tool prior to being released for re-use and disposal.

Deloitte has employed the following methods of PDA protection: 1) forced access PINs; 2) remote wipe in the event of 10 incorrect pin attempts; 3) remote wipe if the PDA is reported as lost or stolen; 4) encryption; and 5) an installed mobile device management tool.

Data Destruction

Policies and practices are in place with regard to the destruction of confidential information and PII that vary depending on type of media on which such information is stored. Deloitte is aligned with the National Institute for Standards and Technology's ("NIST") guidelines for media sanitization. For example, hard disks, CD/DVD, USB drives are required to be wiped using a disk cleaning tool, while tapes are required to be destroyed at end-of-life. Paper containing such information is required to be shredded.

Encryption

Whole-disk encryption has been deployed on Deloitte-issued laptops. Deloitte's laptops have deployed encryption with the 256-bit Advanced Encryption Standard ("AES") algorithm.

Deloitte has deployed encrypted USB drives intended for use in transporting sensitive or confidential data. This encryption method is FIPS 140-2 compliant.

WinZip is installed on all Deloitte-issued laptops. This encryption method is FIPS 197 compliant.

Additionally, Deloitte Internet email gateways are configured to attempt to transmit all email in an encrypted manner, using opportunistic TLS encryption, if the recipient of the transmission can support such encryption methodology. If TLS is enabled on the recipient

email gateway, the email will be encrypted between the Deloitte gateway and the recipient gateway. TLS encryption can also be enforced when agreed with the recipient organization. This encryption method is FIPS 140-2 compliant.

Data in transit is protected by secure TLS using certificates with minimum 2048 bit RSA key and SHA2 signing when using Deloitte secure websites and file transfer services.

Secure File Transfer Protocol ("SFTP") is an available option for the transfer of client data. SFTP securely encrypts and compresses files during transmission. This encryption method is FIPS 140-2 compliant.

Records Management

Deloitte maintains and retains records in accordance with applicable legal and regulatory requirements and professional standards. Specific areas of focus include:

- Facilitating compliance with external requirements and internal policies and practices pertaining to record retention;
- Managing recordkeeping critical to the operation of our business and service to our clients;
- Designing and implementing records management technology, tools, and standard processes;
- Coordinating the proper handling of files on legal hold due to legal, tax or regulatory preservation requirements; and
- Maintaining a strong, compliance-focused records and information management governance organization.